State of California

REFERENCE GUIDE

Continuity Planning for Business (CPB)

v. 2.1

June 4, 1999

Table of Contents

INTRODUCTION

The Department of Information Technology (DOIT) has developed the Year 2000 (Y2K) Continuity Planning for Business (CPB) methodology to assist State Entities in developing plans to reduce the impact of potential Y2K risks on the delivery of services to California citizens. Y2K continuity planning is a broad effort that looks at potential failures in infrastructure, interfaces, data exchanges, and supply chains; the impact such failures may have on business operations; and the strategies to reduce and mitigate those failures.

An essential focus of the continuity planning process is on the provision of mission-critical services to California citizens. This involves understanding which agencies and departments are responsible for those services, and prioritizing the continuity planning development effort accordingly. The State defines a mission-critical service as any service that relates to:

Service	***Description***
Public Safety	Those functions of government that exist to protect the physical well-being of the public as a whole from physical danger
Public Health	Those functions of government that exist to protect the longevity and quality of life for the public as a whole
Law & Justice	Those functions of government that exist to prevent violations of the laws and rules of society by individuals and groups
Environmental Protection	Those functions of government that exist to protect the environment from changes that are detrimental to the existence and continuance of that environment
Human Services	Those functions of government that exist to provide for individuals that are physically, emotionally, financially, academically or intellectually disadvantaged when compared to social norms
Mission-Critical Operations	Other business operations or systems supporting critical service provision including those functions of government that exist to provide vital financial and transportation related services

Throughout the document, we will refer to these as “State mission-critical services.” Given the time and resource constraints leading up to the century event, the emphasis needs to be on creating a statewide business continuity plan to address the continued delivery of State mission-critical services to the citizens of California.

A well-developed continuity plan will maximize the entity's ability to continue to deliver its core services in the event of a significant Y2K disruption. Continuity planning should maintain a

process perspective, shifting the ultimate responsibility for handling the Y2K problem from the IT department to business executives - it is not an IT problem, but rather a business problem.

The CPB methodology encompasses three interrelated components: Risk Reduction, Contingency Planning, and Business Resumption Planning.

- **Risk Reduction** involves targeting certain critical, high-impact risks and designing action steps to reduce or eliminate the risk. The goal is to change the nature of the risk so that it no longer represents a serious threat to business operations.

- **Contingency Planning** involves identifying alternate ways of operating the business process assuming the loss of specific assets and resources normally available to the business operation. Contingency Planning includes the activities and resources required to bring operations back to at least the lowest acceptable level of service delivery, ensuring the delivery of the most critical services until normal operations are resumed. This planning is undertaken in response to a risk that cannot be easily reduced.

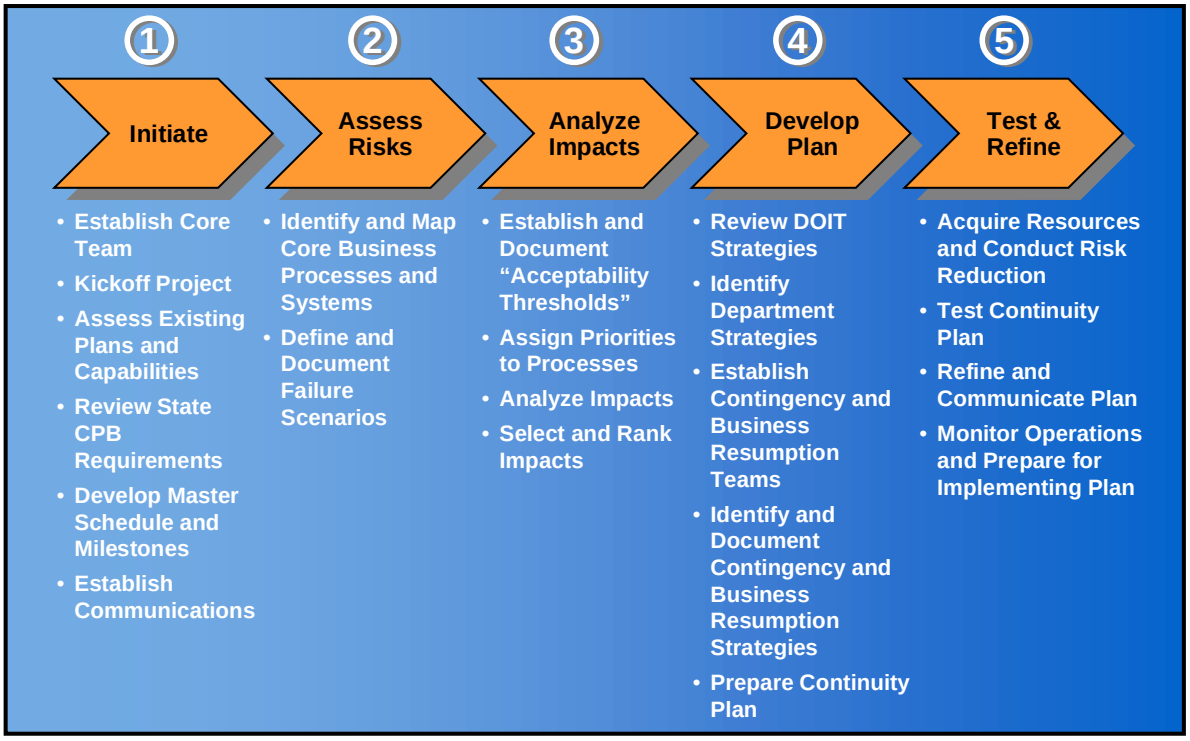
- **Business Resumption Planning** involves identifying the manner in which normal operations are restored. It focuses on the additional efforts that will bring the entity back to normal operating levels. It lists those ADDITIONAL or ALTERNATE resources and/or activities that will bring the entity back from a contingency mode to normal operations, terminating the contingency operations in the process.

Taken as a whole, these represent the documented action items that will improve the ability of a department to prepare for and respond to situations with the greatest potential to affect critical operations.

CPB Methodology Overview

The CPB methodology provides a proven approach to assist State entities in developing a comprehensive Business Continuity Program, in accordance with Governor's Executive Order D-3-99. The methodology is based on industry best practices and lessons learned in the field of business continuity and contingency planning.

Figure 1 - DOIT CPB Methodology



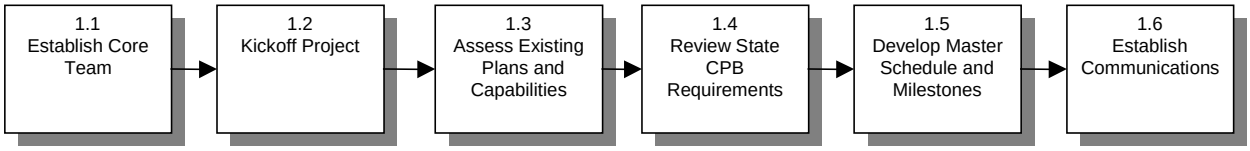
PHASE 1: INITIATE

Overview

The first phase of CPB is the establishment of the framework under which the continuity planning effort will be managed. This framework provides a systematic approach to enable an entity to identify, assess, manage, and mitigate Y2K business process risks, and thereby help to ensure the continuity of the entity's core business services.

The CPB methodology starts with executive-level support from the entity executives in terms of resource allocation and personal involvement. A high-level executive is assigned responsibility for the effort and begins by organizing a core CPB team. The team begins by developing a high-level business continuity planning strategy for the department. The team will also develop a master schedule and establish milestones that must be met in order to complete the plan. Milestones will be directed in part by DOIT, and will be driven by the status of each entity's Y2K compliance efforts. Each entity should develop a plan that focuses on evaluating and addressing the gaps between its existing continuity or contingency plans and the State CPB requirements.

The approach to initiate the CPB process consists of six components, each important in establishing a comprehensive strategy:



1.1 – Establish Core Team

Continuity planning shifts the ultimate responsibility for handling the Y2K problem from the IT department to business executives, as it is an effort requiring a business operations perspective. To facilitate this, the entity should establish core teams to serve as the business continuity work group. The group, which reports to executive management, needs to include representatives from the agency's major business units with expertise in relevant functional areas; business continuity and disaster recovery specialists; and operational analysts.

Establishing the business continuity core teams involves defining roles and assigning responsibilities for leading the planning effort, performing analyses, and developing contingency and resumption plans for each of the core business processes.

Process owners of each core business process should be appointed to lead the development of the continuity plan for their respective areas. Each core team should include representatives with extensive knowledge of the operational procedures necessary to deliver the respective business process. These individuals should be able to clearly define the essential operational activities for their areas, since they will probably be responsible for executing the plan in the event that the entity needs to operate under its continuity plan.

1.2 – Kickoff Project

The CPB effort should start with development of a high-level business continuity planning strategy. Use the initial meeting to get the right parties together to plan for this effort. The meeting should include business function leads and business executives from each core business process. The kickoff serves as both a project initiation and awareness exercise. It should include an executive overview for the agency's executive management team which provides a discussion on the entity's Y2K business risk exposure and current preparedness, and the need for CPB. The CPB strategy should address the project structure, its relationship to the State's and the entity's Y2K program, metrics and reporting requirements, and initial cost and schedule estimates.

1.3 – Assess Existing Plans and Capabilities

The purpose of this step is to inventory existing business continuity, contingency, resumption and disaster recovery plans. It is expected that many of the State entities have already developed components of these plans. The CPB methodology is not intended to void previous planning efforts, but rather should leverage such efforts.

The team should collect, from throughout the entity, any plans and documentation previously developed for business continuity, disaster recovery, systems contingency and other related areas. The inventory should focus on the validity, relevance and overall applicability of the existing plans to meeting the objectives of Y2K CPB. It is likely that existing continuity plans are focused solely on data or computer systems recovery instead of continuity of service delivery.

Considerations for assessing existing plans:

- **Scope:** Identify which systems and business processes are addressed.
- **Validity:** Identify the date the plans were last updated and review to ensure that systems and processes addressed are still valid.
- **Testing:** Assess the feasibility of implementing the plans, including whether they have been tested.
- **Relevance:** Assess plan provision for the continuous delivery of mission-critical services in the event of a Y2K failure, including a failure which could occur externally. A critical factor is the identification of and emphasis on provision of mission-critical services. If this analysis has not been performed, then additional effort will need to be directed at closing that critical gap. This is referenced further in Phase 1 Step 1.4.

1.4 – Review State CPB Requirements

Each entity should review the State requirements (i.e., DOIT requirements and any exiting authorities (e.g., State Emergency Plan, Administrative Orders, etc.)) to identify potential gaps between its plan and the State requirements. Ideally, previous plans should closely match the requirements and phases of the CPB methodology. However, this assessment should identify weaknesses and strengths of existing plans, and determine the extent to which previous efforts map to the State requirements.

- Keep in mind that the CPB methodology is business process-oriented rather than systems-oriented.
- Be aware that the program areas within the entity may have achieved varying levels of continuity planning.

Note: Administrative Orders are available from the Office of Emergency Services (OES) Plans Unit; the State Emergency Plan is available on the OES web site (www.oes.ca.gov) -.

1.5 – Develop Master Schedule and Milestones

To ensure the success of the CPB effort, an entity should develop a project workplan against which to track and measure its CPB progress. Workplans and milestones provide a clear understanding of planned and accomplished progress.

Schedules and deliverables need to be linked to critical stages and deadlines in the statewide Y2K program. DOIT will provide specific milestones and schedules, reflecting completion of the different phases of the CPB process. The master schedule will provide information to enable all stakeholders to see the effort required to complete the plan and will identify the individual roles, responsibilities, and milestones.

1.6 – Establish Communications

Effective communication is essential on any project and, therefore, the core team should establish a communication and reporting process early in the project. This includes communication on policies, procedures, and guidelines for CPB development and reporting.

Project level reporting and communication should be appropriately shared with internal and external stakeholders. To facilitate internal communications, the project team should establish and maintain communications with each business area to ensure their efforts are in line with project goals.

Project reporting tools and procedures should be used to communicate project status to the internal stakeholders. In general, the project team should produce periodic status reports that include accomplishments to date, activities in progress, planned activities, and issues for discussion. This will help increase the level of awareness within the organization and contribute to a sense that potential events are being effectively managed.

Each entity should also establish a regular communication link with the DOIT as well as other relevant stakeholders who are not directly involved with the project on a regular basis, such as other internal stakeholders, other state entities, local, county and federal governments and the private sector. The DOIT will be monitoring and reporting on the status of all mission-critical Y2K continuity efforts and will act as the central repository of information regarding the status and progress made by State entities in ensuring Y2K preparedness.

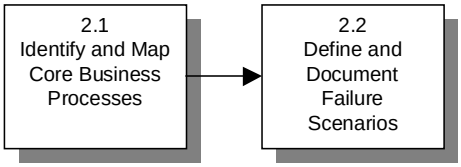
PHASE 2: ASSESS RISK

Overview

Before the entity can develop its continuity plan, it must first identify the risks that threaten the successful delivery of its mission-critical services. This phase (1) establishes a framework to assess risks and aid in the development of a comprehensive plan to mitigate the impact of risks that materialize, and (2) enables the entity to quickly recover its ability to deliver its mission-critical services.

This approach towards risk assessment focuses on ***business processes***, rather than technology-related information systems. A risk assessment based on information systems lacks the comprehensiveness necessary to capture business process risks. To facilitate the comprehensive identification of potential failure points, the entity must take a process-oriented approach, first focusing on the high-level, and then on the details, identifying significant failure points throughout the layers.

The approach for assessing risk using the CPB methodology consists of three components, each important in establishing a comprehensive strategy:



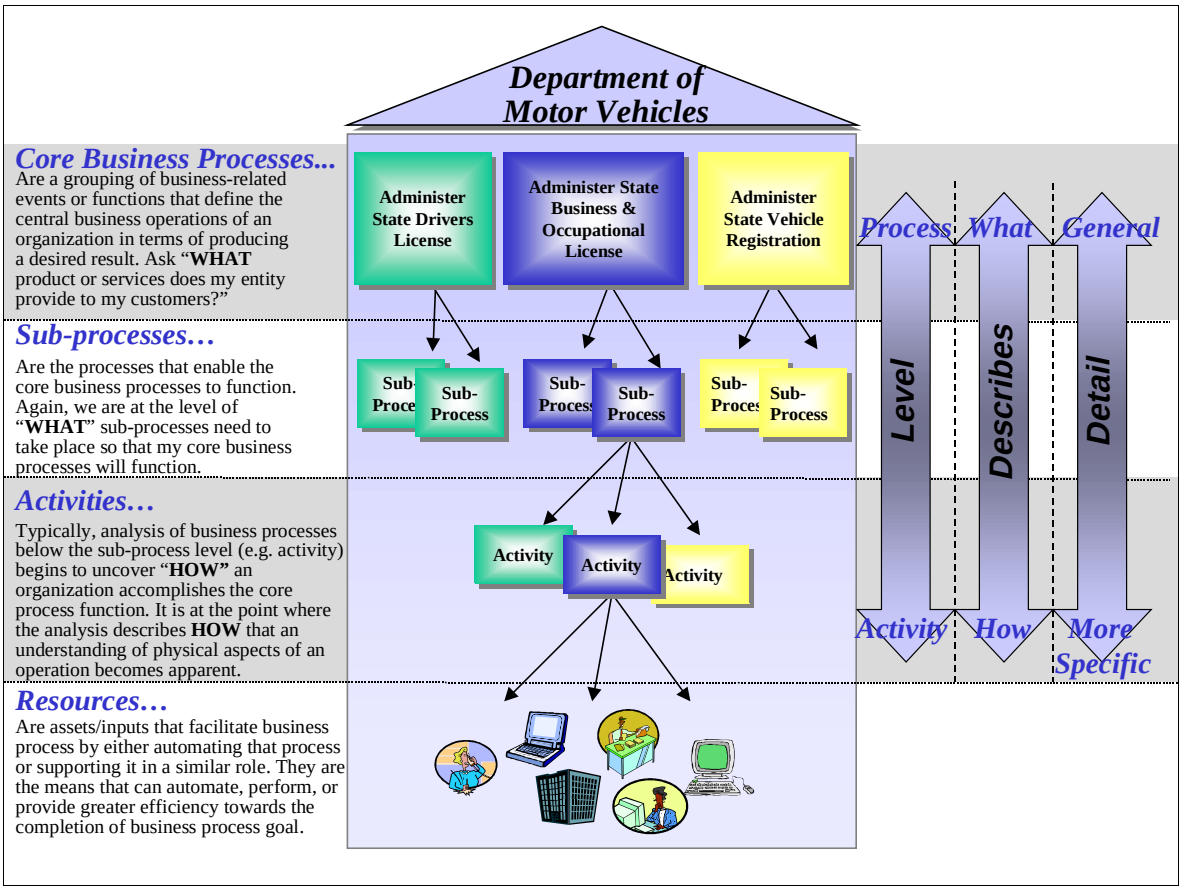
2.1 – Identify and Map Core Business Processes

The framework for risk assessment using the CPB methodology is *process*-centered and *customer*-focused. The entity should first examine its business risks from a *process* perspective and subsequently assess any mission-critical information systems that support its core mission-critical business functions. It is important to remember that continuity planning addresses a business problem, not just an IT problem.

Core business processes, sub-processes, activities, resources and their interdependencies need to be identified and mapped, allowing the entity to identify potential points of failure in its processes and resources.

Figure 2 represents the decomposition of core business processes into sub-processes, activities and resources.

Figure 2



One of the most common approaches used to identify and map the entity's business processes and supporting resources is to hold facilitated workshops attended by all appropriate stakeholders. These stakeholders represent staff from various levels of the organization, typically including business process owners with a broad overview of processes and issues, and subject-matter experts (SMEs) with more detailed knowledge of processes and issues.

2.1.1 Identify Core Business Processes

The basis for the CPB process is a clearly documented understanding of the business processes that support State mission-critical services. To facilitate this, the entity must first define its core business processes. A core business process is typically a grouping of related functions that define the central operations in terms of delivering a product or service. It is important to remember that a core business process is generally not the primary function of a department. Business processes often span different programs, reflecting that a core business process is the delivery of a desired service or product by the entity, not just by one program. The question "**WHAT** products or services does my entity provide to my customers?" is helpful in determining an entity's core business processes.

2.1.2 Identify Sub-Processes and Activities within Core Business Processes

Sub-processes further decompose "what core business processes do" and describe "what it takes to accomplish a core process." The level below the sub-processes represents *activities,* which are the building blocks of sub-processes. Typically, analysis of the activities begins to uncover *how* an organization accomplishes the business process. It is at this point where the understanding of physical aspects of an operation becomes apparent.

2.1.3 Identify Critical High-Level Resources

Notice that in Figure 2, *resources* is the bottom-most layer. Resources generally support business processes at the task or activity level. These resources are mechanisms that facilitate a business process by either automating that process or supporting it in a similar role. They are the mechanisms that help to automate, perform, or provide greater efficiency in the completion of business process goals. Examples of resources include system support resources, infrastructure support resources, suppliers, customers, service levels, or processing cycles.

Resources need to be analyzed to identify potential points of failure. However, the task of identifying resources can become unmanageable unless scope is managed. As many processes and activities may have a large number of supporting resources, listing every resource can result in an overwhelming amount of detail and may hinder progress.

To ensure identifying the critical resources results in useful data, the entity will need to make sure the level of detail is appropriate. A useful approach is to group resources into categories or resource classes that have similar levels of risk. This will allow the entity to address resources with similar risk characteristics as a combined "risk class", and minimize the level of detail required. Entities should take inventory of only those resources that help support the delivery of mission-critical processes.

2.1.4 Map Core Business Processes

In this activity, the entity needs to clearly and accurately capture all of the business processes that it performs to support State mission-critical services, as well as the systems that support those business processes.

One of the most effective ways to document the flow of business processes and supporting information systems is to use process mapping or decomposition. Process mapping diagrams and their supporting documentation can be used to show business processes and information requirements at any level of detail.

2.1.5 Analyze Interdependencies as they Relate to State Mission-Critical Services

Again, emphasis and priority should be given to State mission-critical services. Once the mapping of the interdependencies between the various levels of processes and the supporting systems has been performed, use the mapping diagrams to help ***analyze*** the interdependencies and identify potential failure points.

Numerous approaches exist to analyze the interdependencies. Either a 'top-down' or 'bottom-up' approach will assess the underlying or related processes/systems that would be impacted by a failure at a certain point. Whether the point of failure is at the process, sub-process, activity, or resource level, entities should think about the processes that would be affected by either a "trickle-down' or 'upwards spiraling' effect. That is, look above and below the failure point to determine what other areas may be impacted by the failure.

2.1.6 Establish and Document Process/System Metrics to Monitor Core Business Processes and their Performance Over Time

It is critical that an entity captures process and system metrics to determine if failures were Y2K induced. These metrics can serve as a benchmark to help determine the trigger point for contingency plans.

Each business area should define the way operations are measured to gauge performance levels. Typical examples include cycle time, item process count, error rates, etc. Similarly, system performance metrics should be established and documented. Examples of these include availability, transaction processing standards, response time, etc.

2.2 – Define and Document Failure Scenarios

Developing Y2K failure scenarios entails assessing the entity's business vulnerabilities and their impacts, and defining Y2K risk scenarios. These risk scenarios will be used to analyze the impact on the entity's processes. Some examples of potential failure scenarios include the loss of:

- **Access**: to information systems, data, documentation, communications, etc.
- **Utilities**: electricity, water, gas
- **Facilities**: corporate headquarters, field offices, etc.

2.2.1 Define and Document Potential Failure Scenarios

Define potential Y2K-related failure scenarios. For example, assume the loss of all mission-critical information systems due to post-implementation failures or delays in remediating and testing. Consider the possibility that Y2K date problems may be encountered earlier than expected; address the potential disruption of essential infrastructure services. Focus agency business continuity and contingency planning efforts on likely failure scenarios.

2.2.2 Quantify Likelihood of Failures

To better prioritize and allocate activities in contingency and continuity planning, the entity needs to determine the likelihood that failure modes will occur. The likelihood of occurrence can be represented as a numeric value or a ranking of high, medium, and low, determined during a brainstorming session when all appropriate stakeholders are present.

2.2.3 Identify Impacts or Effects of Failures

Here the entity will perform an impact assessment of identified risks. For each identified failure and/or risk, determine the overall impact or effect that particular failure/risk could have on the business process. This analysis should include mapping of the failure/risks against the core processes and sub-processes. The impact of the risk/failure on a business process can also be described as high, medium or low.

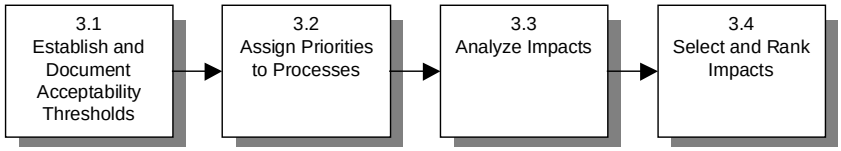
PHASE 3: ANALYZE IMPACTS

Overview

The objective of this phase is to analyze the impacts that risks have on an entity's ability to deliver its mission-critical services. Impact analysis is a systematic way of prioritizing those impacts on the entity that pose the greatest threat to the delivery of its mission-critical services.

An important aspect of impact analysis is the establishment of minimum acceptable levels of operation because it establishes targets for interim operations that allow business functions to continue. This analysis acknowledges that certain disruptions can be tolerated for some period.

The approach to impact analysis using the CPB methodology consists of four components, each important in establishing a comprehensive strategy:



3.1 – Establish and Document Acceptability Thresholds

Acceptability thresholds define the level of service and length of time at which a significantly degraded core business process can operate and still provide an acceptable level of service. These thresholds need to be defined by the business process owners, but may be influenced by legislative or similar mandates. The thresholds defined for each entity serve as the foundation to rank and prioritize corrective actions. There are two criteria used to quantify acceptability thresholds: minimum acceptable level of service, and maximum acceptable outage. These criteria are shown in Figure 3.

Each entity needs to define the minimum acceptable level of service or output for each core process and estimate its maximum acceptable outage. These should be based on the established and assessed metrics for core processes during normal conditions. The process owners need to define this level for their respective processes.

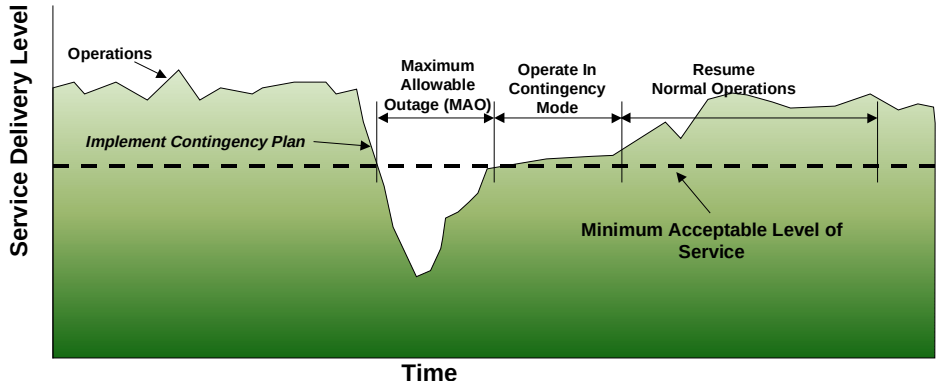
The **minimum acceptable level of service** is a metric reflecting the lowest threshold of service that the entity can provide for each core business process. Contingency plans will attempt to restore operations to this minimum level or prevent service from falling below this level. An example of a minimum acceptable level of service is as follows:

> *Agency XYZ normally processes 100 ABC mission-critical transactions each day. The ABC business process owners have evaluated the typical transactions processed each day and concur that only 45 ABC transactions require a 24-hour turnaround. The remaining 55 transactions, the process owners decide, are of much lower priority and can be processed*

within a few weeks. The minimum acceptable level of service for the ABC process is 45 transactions per day.

Continuity planning efforts for the Agency XYZ example would focus on actions necessary to process the 45 ABC transactions each day. The entity must also define the period of time for which this degraded, manual service level can be tolerated.

Figure 3 - Acceptability Thresholds



Maximum Acceptable Outage (MAO) is the maximum amount of time that an entity can go without certain core business processes before significant impacts occur. The MAO should be determined for each system or sub-process that impacts a core business process. Continuing the example from above:

Agency XYZ processes its ABC transactions using Computer System 1. The ABC business process owners have identified that the maximum amount of time Computer System 1 can be out of service is two days. The maximum acceptable outage for Computer System 1, which supports the ABC transactions, is two days.

Planning efforts would focus on how to process the ABC transactions within two days using either Computer System 1, manual processes, or other workarounds.

3.2 – Assign Priorities to Processes

Entities should focus their efforts on mitigating the risks that most threaten their ability to deliver certain critical services. The purpose of this step is to determine which processes and systems are most critical to the successful delivery of the entity's mission, especially those supporting the State's mission-critical service delivery.

Business priority is determined by combining the following two factors:

- Importance to Business Operations
- Susceptibility to Y2K Failure

Review the outcomes from the business process analysis, and the outcomes from the preceding step (MAO), as well as the results from the risk and failure analysis activities. These will serve as inputs into the criticality analysis, which provides an objective framework for prioritizing processes/systems.

Identify the appropriate criteria for filtering out the processes/system that are truly most important from a State mission-critical perspective. Consider factors such as complexity, risk level, mission-criticality, etc. Include any reasonable characteristic that helps you further prioritize and rank your critical processes.

Applying the metrics deemed most relevant by business process owners, the criticality analysis will assist an entity in sorting out which processes are most important from a State mission-critical perspective. The result of this analysis is a ranking of processes and systems by overall criticality.

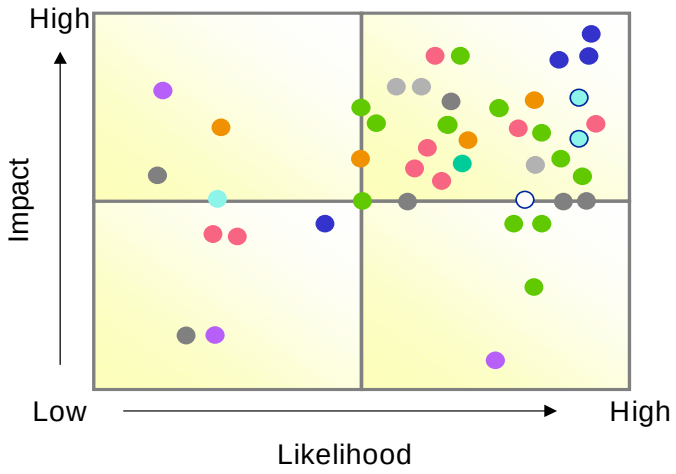
3.3 – Analyze Impacts

The main purpose of this step is to analyze the impacts of the risks identified and documented in Phase 2. Impact analysis will help the department and other stakeholders determine the effects specific risks have on certain processes. It will help determine which impacts are acceptable and which are not. It also allows the department to evaluate if the cost of mitigation efforts corresponds to the value of the disruption. Various tools can be used to systematically and consistently rank and prioritize risks and impacts.

Impact is the assessed measure/value of the consequences from the realization of a risk. Therefore, in performing impact analysis the focus should be on assessing the impact or consequence the realization of a risk will have on the entity's core business processes, as well as the relative rank of those impacts.

An output from this phase will be a clear understanding of the risks that face the entity. A graphical representation of the relative impact and likelihood of each risk (as shown in Figure 4) can help the entity focus subsequent analysis and resources on those risks which warrant action.

Figure 4 - Impact Analysis Scattergram



3.3.1 Analyze Impacts In Relation To Likelihood vs. Severity of Impact

Classify and categorize each risk by its impact and probability of occurrence. Categorization occurs by assigning a "priority category" (low, medium, high) to each identified impact. Use simple risk assessment tools, such as the matrix in Figure 4, to help you assess and graphically map the risk and its associated impact. The risk assessment tool can help you categorize risks that require a common management approach.

Business process owners need to define the priority categories. Examples of priority categories are illustrated below:

Effect on Business Operations		Financial Scope of Problem		Effect on Public	
High	Complete or nearly complete shutdown of services	Large	Impact value of $1 million or more	Immediate	Impact is evident to public within 1 to 5 days after failure
Medium	Significant loss of quality and/or quantity of services	Medium	Impact value between $100,000 - $999,999	Delayed	Impact evident to public within 6 days or longer after failure
Low	Little or no impact on service	Small	Impact value of $100,000 or less	None	No impact to public

Part of the analysis involves identifying the two types of risks: moveable and static. A moveable risk can be reduced by addressing it before impact occurs. A static risk cannot be reduced, so a contingency plan should be developed for it.

3.3.2 Analyze Impacts in Relation to Likelihood of Occurrence vs. Level of Impact

Impacts can vary in scope in that they can affect different levels of the entity. Document WHERE in the entity the impact will occur. Is there a difference between the impact at the business unit level and the enterprise level? For example, staff impacts or shortages may not be critical at an individual business unit level. They may believe they can get adequate backup. However, if all

business units have the same problem at the same time, the impact to the enterprise would be more severe. This kind of analysis can result in a more in-depth understanding of the impacts and validate the impact level(s) determined in earlier steps. This can be used to indicate where and to what degree the realization of a risk will impact selected LEVELS of the organization. Considerations in this analysis may include:

- The level of impact on business operations at selected levels (business unit, division, organization)
- The scope of the problem and the number of customers/stakeholders affected (the more affected, the greater the impact)
- Whether failure would cause an immediate effect, delayed effect, or no effect on the customer

3.3.3 Analyze Impacts in Relation to Likelihood vs. Cost of Prevention/Mitigation

In this activity, perform a cost-benefit analysis of mitigation efforts versus costs. The following needs to be done:

- Identify appropriate mitigation efforts for each identified impact.
- Develop cost estimates for risk mitigation activities. This will be used in the next activity.

3.4 – Select And Rank Impacts

Impacts have many characteristics and may affect different parts of the entity in different ways and at different levels of severity. To make informed decisions in allocating scarce resources to where they may have the greatest positive impact on the entity and enable it to continue operations, an entity must select appropriate reduction and mitigation strategies.

Risks should be prioritized on the basis of whether they involve mission-critical processes, have large financial impacts, etc. This will result in a list which can be used to guide the mitigation strategy that determines where the entity's scarce resources should be allocated.

By using the outcomes from the risk assessment and the criticality analysis as inputs, the entity can group and prioritize risks, processes, and supporting systems in categories. These categories will enable an entity to determine the appropriate mitigation/risk reduction strategy, or if a contingency plan should be developed. Typical categories include:

Priority Category	Business Impact Description
Category 1: ***Catastrophic***	The impact of this risk would have a **catastrophic effect** on operations. Examples of this include prolonged disruptions to the core business processes which provide a critical service to the citizens of California. It would also include any core business process that another department or agency relies upon to provide services to the citizens of California.
Category 2: ***Severe***	The impact of this risk would have a **severe effect** on day-to-day operations. Operations may still be able to be performed for a limited period of time. However, losing these core business processes for more than a minimum length of time would cause a significant degree of disruption and ultimately have a catastrophic effect. "Workarounds" for these core business processes would cost a significant amount of money or take a great deal of time.
Category 3: ***Sustainable***	The impact of this risk would have a **sustainable effect** on day-to-day operations. Some of the tasks carried out within this category could be performed manually and "workarounds" would not entail a significant amount of effort or cost. Operations could continue for some time prior to full resumption.
Category 4: ***Inconvenient***	The impact of this risk would not have any significant effect on operations. Examples of these include those business processes which do not add a great deal of value to operations and hence will have little effect if they are not functioning optimally. Infrequent manual tasks fall into this category.

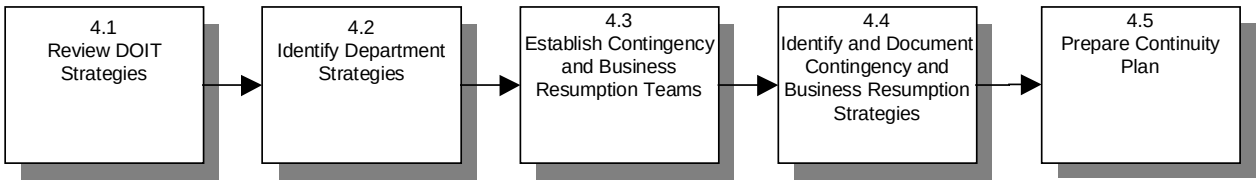
PHASE 4: DEVELOP PLAN

Overview

Now, it's time to pull together all the data gathered and analyzed in prior phases and develop the plan. The Continuity Plan will address three key areas: (1) risk reduction to move risks out of the most critical category, if possible, (2) contingency planning for processes that support State mission-critical business functions, and (3) business resumption planning to ensure the continuity of State mission-critical services. Together, these three components represent the activities necessary to adequately ensure the continuity of the State's most critical operations and/or the resumption of such operations within the timeframes necessary after a potential Y2K disruption.

You now have knowledge of the most important risks in terms of their severity and impact on provision of mission-critical services. The next steps involve identifying how the organization will approach the management of these critical risks and documenting the activities and resources necessary to respond to the risks which cannot be avoided.

The approach to developing the plan using the CPB methodology consists of five components, each important in establishing a comprehensive strategy:



4.1 – Review DOIT Strategies

To assist State entities in identifying their State mission-critical processes, DOIT has defined categories of mission-critical services. The priorities set by entities must allow for the continuity of State mission-critical services in each of the defined categories. This includes reduction and mitigation of risks impacting associated business processes.

4.1.1 Review State Mission-Critical Definition

Confirm that each identified mission-critical process is consistent with the State mission-critical services definition. The mission-critical categories are defined in the Introduction.

4.2 – Identify Department Strategies

Each department or organization has unique situations and requirements that must be considered when developing the continuity plan. This step involves identifying and documenting which

risks and situations warrant deployment of scarce resources to accommodate either reduction/prevention or contingency strategies.

4.2.1 Review Prioritized Impacts

Impact analysis and prioritization performed in Phase 3 should be reviewed to determine which processes warrant attention. Any changes or consolidations can be made at this time, but the focus should be on understanding where similarities exist between the ranked impacts so that resources and solutions can be targeted toward risk reduction or elimination that would benefit more than one business area at a time.

4.2.2 Coordinate with Other Emergency Response Agencies

Each entity should understand and consider the emergency response services for which they are responsible to ensure appropriate coordination with other federal, state or local entities that may be impacted. For example, OES or a county's emergency response center may have responsibility for coordinating resumption of certain infrastructures.

4.2.3 Identify Risk Management Strategies

Risk reduction and elimination - Given the risks confronting mission-critical operations, each risk should be evaluated to determine if there are reasonable ways to make failure of the operation less likely or prevent the failure altogether. For example, if one of the risks involves the inability to deliver the necessary staff and skills mix, cross training staff in multiple functions might substantially alleviate the risk.

Risks that cannot be reduced or eliminated - For those risks that cannot reasonably be reduced, identify ways in which the risk will be managed to allow business operations to continue within an acceptable range of performance. Considerations during this analysis include the need to direct resources toward prevention and reduction of impacts in those areas most directly related to provision of State mission-critical services.

4.3 – Establish Contingency and Business Resumption Teams

The purpose of this step is to establish the teams that will be responsible for managing the implementation of contingency and resumption plans. These teams must be able to respond to a wide range of operational problems, including failures of systems originally thought to be remediated and tested, failures of external systems and data exchanges, infrastructure failures and other disruptions. Members of the team will likely have been involved in the development of the strategies in Activity 4.2.

4.3.1 Establish a Team for each Core Business Process

Identify the teams who will be responsible for implementation of the contingency and business resumption plans. All team members must have the training and the ability to perform implementation tasks, and each member should have an alternate who is equally qualified.

Identify any special skills needed and any particular individual(s) with knowledge of the specific processes or functions needed for the team to be successful.

4.3.2 Define and Assign Team Roles and Responsibilities

Define roles and responsibilities of each team member, including who will be responsible for planning, implementing, testing and validating the contingency and business resumption plans for each business process. This should include who will be responsible for public communications and coordinating with outside stakeholders.

4.3.3 Define and Document the Roles, Responsibilities, and Authority for Taking Action during the Failure Scenario

Coordination of activities and communication is essential for the successful execution of any contingency and/or resumption plan during a disruption. As events unfold, it may not be possible to follow specific, detailed steps included in the plan. When this occurs it is important for the team to have the communication channels and structure in place to allow the rapid response and resource deployment needed to manage the event. In addition to roles and responsibilities, this information includes definition of the escalation sequence for resource deployment and procedure modification and identification of any approvals needed to activate the plans and redirect operational activities and resources. This process includes mapping out how the business process owners are to be involved during execution of the contingency and resumption plans.

4.3.4 Identify Resources Necessary to Execute the Plans

Include resources necessary to perform any identified activities required prior to the failure, such as copying files, generating reports or preparing manual forms, as well as the resources required to return to normal operations. These resources should also include special materials or staff needed to operate using alternative procedures. The purpose of this activity is to avoid resource shortages, causing an inability to meet established timelines.

4.4 – Identify and Document Contingency and Business Resumption Strategies

The purpose of this step is to identify and document the organization's strategies for maintaining the viability of its most critical business functions, as well as strategies for returning to normal operations. Typically, there are many different approaches that can be taken to maintain and resume business operations. During this step, the Contingency and Business Resumption Team(s) will design, develop and select strategies that provide for recovery to the minimum service level within the recovery time objective and eventually return the business process to normal operations.

4.4.1 Identify Contingency and Resumption Scenarios

Determine the failure or disruption scenarios to be documented. The general scenarios were developed during Phase 2, Assess Risk. At this time, the failure scenarios should be examined to

determine how the failure will be managed and adequate business operations maintained and subsequently restored. These scenarios should be Y2K-specific and include situations that are likely to occur and within the department's ability to react. For example, planning for localized utility disruption is reasonable, while scenarios indicating nationwide power failures are too broad.

4.4.2 Develop Contingency and Resumption Alternatives

Identify and document alternative approaches to address the failure of State mission-critical business processes and the restoration to normal business operations. This information should be developed for each failure scenario and affected critical business process. Alternative procedures must be considered and developed, as the contingency alternatives need only meet the minimum acceptability thresholds, not provide for completely seamless operations. For example, establishing fully redundant systems capabilities would not be warranted if manual procedures and staff could keep information flowing adequately within the business process to meet short-term, acceptable degraded operational targets.

4.4.3 Assess Costs and Benefits of Identified Alternatives

The different alternatives will require varying mixes of resources and procedures. These alternatives must be evaluated on the basis of the expected cost of each compared to the benefit of the services maintained. The cost/benefit tradeoff must be able to pass the reasonableness check, and should be validated by business executives.

4.4.4 Select the Preferred Contingency/Resumption Strategy

Select a strategy that is practical, cost-effective, and appropriate to the organization. In addition, the alternatives and strategies should provide a high level of confidence in the contingency strategy and recovery capability.

4.5 – Prepare Continuity Plan

Entities must identify strategies and document action plans for maintaining acceptable levels of critical business operations. The Continuity Plan encompasses three elements: Risk Reduction, Contingency Planning and Business Resumption Planning. Taken as a whole, these represent the actions necessary to ensure an entity’s ability to prepare for and respond to situations with the greatest potential threat to critical operations.

4.5.1 Prepare Risk Reduction Plan

Strategies identified in Activity 4.2, Identify Department Strategies, are translated into specific action steps to accomplish appropriate risk reduction. The plan should be grouped by risks to be reduced. Each detailed activity should indicate the timeframe for action; business process impacted; responsible party; and resources required.

4.5.2 Prepare Contingency Plans

Entities must develop contingency plans to ensure the minimum acceptable level of service for each core business process. Consideration must be given to any potential Y2K failure that could have a significant negative impact on the delivery of mission-critical services.

4.5.3 Prepare Business Resumption Plans

Each entity must develop resumption plans to ensure operations are restored to normal levels in an orderly fashion. The plan should be grouped by critical business process. Within each scenario, the detailed activity should indicate the required timeframe for action; business process impacted; responsible party; and resources required.

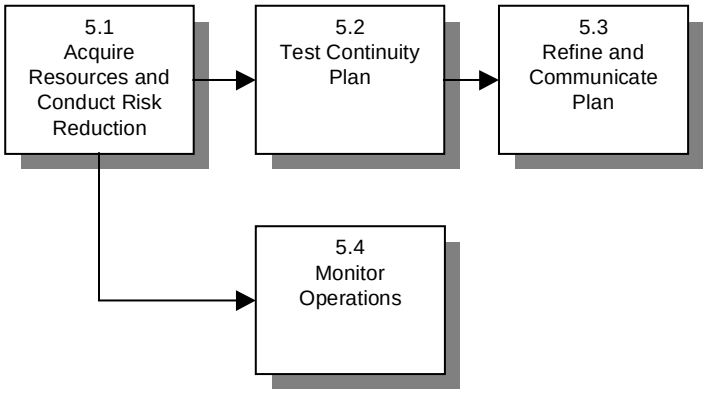
PHASE 5: TEST AND REFINE

Overview

This phase focuses on the testing and refinement of the continuity plans. Testing of continuity plans helps to determine if the plans are realistic, practical, and executable. It is important for State entities relying on previous continuity plans to validate and test those plans to ensure they are up to date, and address service continuity from a process perspective.

Executing the tests and measuring results against pre-defined metrics will validate the plan and indicate whether all scenarios and vulnerabilities have been anticipated, as well as provide data on the areas of the plan that require improvements. Finally, metrics must be established to allow the entity's staff to detect when a failure occurs and a response is required. Contingencies outlined in the continuity plan should be communicated to personnel that support, either directly or indirectly, the core business processes of the entity.

The approach to prepare, test and refine the plan using the CPB methodology consists of four components.



5.1 – Acquire Resources and Conduct Risk Reduction

This step includes the mechanics for implementing the entity's continuity plan. Implementation activities for the continuity plan provide reassurance that the paper-based analysis and planning conducted so far can translate into actions that restore business capabilities. Implementation can be performed at various levels, from initial pilot studies to full-scale implementation of the continuity plan.

In Phase 4, entities should have identified and documented the required resources for the continuity plan. Now those staffing requirements must be negotiated and secured to ensure that there will be adequate emergency response staff to implement the continuity plans.

The plan should include procedures for the overall plan administration and execution. Business unit managers should be heavily involved in this phase to ensure their ownership of the program once the implementation is complete.

Next, execute the risk reduction strategies documented during Phase 4. Remove as much uncertainty from your resource mix as is reasonably possible. This may include altering the schedule of certain activities to move them out of the Y2K timeframe.

5.2 – Test Continuity Plan

Testing of the continuity plan provides reassurance that the paper-based analysis and planning conducted so far translate into effective or intended results. Tests should be conducted for those scenarios and critical business processes that are most likely to occur. Staff training and education is important and begins during this phase.

The use of a phased approach for plan testing begins with small, easily defined pieces of the plan and gradually progresses to tests of major portions of the plan. By building up to the larger, more comprehensive tests, the continuity teams can benefit from the early successes, gain knowledge and experience in the testing process and more easily isolate plan weaknesses.

5.2.1 Develop Test Plan and Schedule

Develop scenarios that are applicable to the functions or services provided, and reflect likely failure scenarios. Using the documented scenarios and the test requirements, develop a test plan. The documented test plans should include the test objectives, test approach, required resources as gathered during the above step, test schedules and locations, test procedures and the expected results and exit criteria. If applicable, use a resource inventory list to determine those additional continuity plan resources you might need to acquire.

It may be necessary to restrict the scope of the testing effort to focus on the continuity plans for high-priority core business processes. Also, the test plan should include a test strategy and schedule that reflects incremental complexities in the test process.

5.2.2 Conduct Training

The objective of this activity is to train the staff on the required procedures and activities in the event of a disruption. It is extremely important that operational personnel be trained in the execution of contingency and resumption procedures. This ensures that they will be familiar with their roles and responsibilities in the event the plans need to be activated. Outline activities that will allow them to rehearse the situation in a real-world environment.

Consider the following types of rehearsal:

Desktop exercise: In the desktop exercise, the manager responsible for implementing a continuity plan will be advised of a hypothetical situation. The manager, or his designee, will then use the plan to work out a response to the situation. The manager will answer questions that relate to the availability of trained staff and adequacy of the facilities and machines, and whether

necessary forms and supplies are on hand. Adjustments will be made either to the plan or to the particular environment during this phase should any part of the plan fall short of its objective.

Simulation: Actual simulation takes the desktop exercise a step further. In simulation testing, a component or office (or part of an office) will conduct real business as if in a disrupted operational situation. The simulation will be thorough enough to assure the component manager that on-site personnel can handle the work, the necessary training has been conducted or scheduled, needed supplies are available, and the facility can be adapted to the contingency. At this point, any inadequacy in the plan or the office's preparation will be remedied in advance of an actual contingency situation.

5.2.3 Execute Tests and Document Results

The purpose of this activity is to execute the tests developed to validate the contingency and resumption plans. This task should also validate that the test site is adequately equipped with the resources needed to execute the plans.

The test should simulate actual procedures as closely as possible. This will allow the team to deal with a realistic level of uncertainty and make decisions in an unstructured environment.

5.3 – Refine and Communicate Plan

Once the plan has been tested, it should be refined based upon any issues highlighted in the testing exercises. Things to consider include:

- Does the plan adequately address the business process needs and requirements?
- Are the plan components comprehensive enough to allow for all types of contingencies and situations?

Weaknesses that have been highlighted must be addressed in this step. Consider and implement alternatives to the continuity plan components to mitigate incumbent risks. Alternatives to the continuity plan components should be approved by the executive management team before being implemented and re-tested to validate their appropriateness.

5.3.1 Validate/Improve Plan Components

Results of the test should be used to improve the continuity plan. Additionally, a quality assurance review of the plan can help validate that necessary elements are accounted for. The validation procedure should stress flexibility and adaptability, and capitalize on lessons learned from mishaps experienced in testing. Overall, the entity should ensure that the plan adequately supports the respective core business process.

5.3.2 Communicate Readiness and Preparation

The objective of this activity is to perform outreach by communicating the readiness of the continuity plan to stakeholders, as well as the roles and responsibilities of the individuals responsible for implementing the plan. Inform them of the inputs and outputs to the plans, the interdependencies, and which actions are triggers for activating the contingency and resumption plans. Inform personnel of acceptable behavior should unplanned events occur.

5.4 – Monitor Operations and Prepare for Implementing Plan

This step includes defining the manner in which business processes and general operations are monitored to detect when a failure occurs. To a great extent, this occurs as a part of the normal business management process. Every manager needs to verify that the required work is being accomplished within the appropriate timeframe. To the extent this normal monitoring includes the failure scenarios and trigger events documented in the Continuity Plan, additional effort is not required.

It is important for process owners to be aware of the contingency plan trigger events for their operational areas. If they were not involved in development of the contingency plans for their areas, the internal communication channels must provide for the information flow to these individuals.

It is important to remember that not all disruptions immediately constitute an emergency situation. For example, in the case of a power outage, critical business operations might be capable of sitting idle for a short time, giving the utility provider an opportunity to restore service. Or may be the processes can continue operating through backup generator power for a period of time likely to exceed the event duration. It may be that full contingency operations don't occur until after power has been disrupted for several hours. These details are included as part of the MAO analysis of the business processes.